Improved Asymptotic Key Rate of the B92 Protocol

Ryutaroh Matsumoto*
*Department of Communications and Integrated Systems, Tokyo Institute of Technology, 152-8550 Japan

***Abstract*—We analyze the asymptotic key rate of the single photon B92 protocol by using Renner's security analysis given in 2005. The new analysis shows that the B92 protocol can securely generate key at 6.5% depolarizing rate, while the previous analyses cannot guarantee the secure key generation at 4.2% depolarizing rate.**

I. Introduction

The B92 quantum-key-distribution (QKD) protocol [2] has remained less popular than the famous BB84 protocol [1], while both protocols provide the unconditional security. One plausible reason for the unpopularity is that the B92 is weaker to the channel noise than the BB84. Specifically, the BB84 with the standard one-way information reconciliation can generate secure key over the depolarizing channel at depolarizing rate 16.5%, while the previous security analyses of the B92 cannot guarantee the secure key generation at depolarizing rate 3.5% [8], 3.7% [4] or 4.2% [7].

The conventional security analyses of the B92 [4], [7], [8] involved many inequalities, and the tightness of those inequalities was not explicitly discussed. We cannot exclude the possibility that the B92 protocol can securely generate key at depolarizing rates over 4.2%. On the other hand, the asymptotic secure key rate in [7], [6] is expressed as the minimum of conditional quantum entropy over a certain set of bipartite quantum states. By using the convex optimization technique, we can completely remove careful manipulation of many inequalities, which could underestimate the secure key rate. In this paper we reformulate the asymptotic secure key rate formula as a convex optimization problem, and compute the rate without any manipulation of inequalities directly by a numerical optimization procedure. As a result, we show that the B92 protocol [2] without noisy preprocessing [7] can securely generate key at 6.5% depolarizing rate.

II. New Security Analysis of the B92 Protocol

In this section, we present a new formula for the asymptotic key rate of the B92 protocol, based on Renner's security argument [6]. Firstly, we fix notations. Let $\{|0\rangle, |1\rangle\}$ be some fixed orthonormal basis of a qubit. In the B92 protocol [2], Alice sends the quantum state

$$|\varphi_j\rangle = \beta|0\rangle + (-1)^j\alpha|1\rangle, \tag{1}$$

for $j = 0, 1$, where $\beta = \sqrt{1-\alpha^2}$, and $0 < \alpha < 1/\sqrt{2}$. For convenience of presentation, we also define

$$|\bar{\varphi}_j\rangle = \alpha|0\rangle - (-1)^j\beta|1\rangle.$$

We can see that $\{|\varphi_j\rangle, |\bar{\varphi}_j\rangle\}$ forms an orthonormal basis of a qubit.

On the other hand, we can express a qubit channel as follows. Define the three Pauli matrices σ_x, σ_y, and σ_z as usual. Then a qubit density matrix ρ can be expressed as [5]

$$\rho = \frac{1}{2}\left(I + x\sigma_x + y\sigma_y + z\sigma_z\right),$$

where $x, y, z \in \mathbf{R}$ and $x^2 + y^2 + z^2 \leq 1$. The vector (x, y, z) is called a Bloch vector. The qubit channel $\mathcal{E}_B$ from Alice to Bob can be expressed as a map between Bloch vectors by

$$\begin{pmatrix} z \\ x \\ y \end{pmatrix} \mapsto R\begin{pmatrix} z \\ x \\ y \end{pmatrix} + \vec{t}, \tag{2}$$

where

$$R = \begin{pmatrix} R_{zz} & R_{zx} & R_{zy} \\ R_{xz} & R_{xx} & R_{xy} \\ R_{yz} & R_{yx} & R_{yy} \end{pmatrix}, \quad \vec{t} = \begin{pmatrix} t_z \\ t_x \\ t_y \end{pmatrix}. \tag{3}$$

Define

$$|\Psi\rangle = \frac{|0\rangle_A|\varphi_0\rangle_B + |1\rangle_A|\varphi_1\rangle_B}{\sqrt{2}}.$$

As in [8], we also define the four POVM

$$F_0 = |\bar{\varphi}_1\rangle\langle\bar{\varphi}_1|/2, \tag{4}$$
$$F_1 = |\bar{\varphi}_0\rangle\langle\bar{\varphi}_0|/2, \tag{5}$$
$$F_{\bar{0}} = |\varphi_1\rangle\langle\varphi_1|/2, \tag{6}$$
$$F_{\bar{1}} = |\varphi_0\rangle\langle\varphi_0|/2. \tag{7}$$

After passing the quantum channel $\mathcal{E}_B$ from Alice to Bob, $|\Psi\rangle\langle\Psi|$ becomes

$$\rho_{1,AB} = (I \otimes \mathcal{E}_B)|\Psi\rangle\langle\Psi|. \tag{8}$$

In a quantum key distribution protocol, the state change $\mathcal{E}_B$ is caused by Eve's cloning of the transmitted qubits to her quantum memory. The content of Eve's quantum memory is mathematically described by the purification $|\Phi_{1,ABE}\rangle$ of $\rho_{1,AB}$. Let $\rho_{1,ABE} = |\Phi_{1,ABE}\rangle\langle\Phi_{1,ABE}|$.

In addition to Eve's quantum memory, she also knows the content of public communication over the classical public channel between Alice and Bob. For each transmitted qubit from Alice to Bob, the public communication consists of 1-bit information indicating whether Bob discards his received qubit or not. We also have to take it into account. We shall represent the public communication by a classical random variable P that becomes 1 if Bob discards his qubit and 0 otherwise. So, $P = 0$ when Bob's measurement outcome is F_0 or F_1, and $P = 1$ when Bob's measurement outcome is $F_{\bar{0}}$ or $F_{\bar{1}}$.

On the other hand, in the B92 protocol, Bob performs the measurement specified by Eqs. (4)–(7). Alice and Bob keep

their a qubit if and only if its measurement outcome is F_0 or F_1. Otherwise it is discarded and is not used for generation of secret key. This is mathematically equivalent to set Alice's bit to 0 if the measurement outcomes is $F_{\bar{0}}$ or $F_{\bar{1}}$. Therefore, from Eve's perspective on Alice's classical bit, the joint state between Alice and Bob after the selection by measurement outcomes is equivalent to

$$\begin{aligned}\rho_{2,ABEP} &= (I_A \otimes \sqrt{F_0} \otimes I_E \rho_{1,ABE} I_A \otimes \sqrt{F_0} \otimes I_E \\ &\quad + I_A \otimes \sqrt{F_1} \otimes I_E \rho_{1,ABE} I_A \otimes \sqrt{F_1} \otimes I_E) \otimes |0\rangle_P\langle 0|_P \\ &\quad + |0\rangle_A\langle 0|_A \otimes (\sqrt{F_{\bar{0}}} \otimes I_E \mathrm{Tr}_A[\rho_{1,ABE}] \sqrt{F_{\bar{0}}} \otimes I_E \\ &\quad + \sqrt{F_{\bar{1}}} \otimes I_E \mathrm{Tr}_A[\rho_{1,ABE}] \sqrt{F_{\bar{1}}} \otimes I_E) \otimes |1\rangle_P\langle 1|_P.\end{aligned}$$

Observe that the state change from $\rho_{1,ABE}$ to $\rho_{2,ABEP}$ is a trace-preserving completely positive map.

Remark 1: Alternatively, by using the more usual approach to model a quantum state after selective measurement, one can also regard the quantum state after having Bob's measurement outcome F_0 or F_1 as

$$\begin{aligned}&\frac{1}{(F_0+F_1)\mathrm{Tr}_A[\rho_{1,AB}]}(I_A \otimes \sqrt{F_0} \otimes I_E \rho_{1,ABE} I_A \otimes \sqrt{F_0} \otimes I_E \\ &+ I_A \otimes \sqrt{F_1} \otimes I_E \rho_{1,ABE} I_A \otimes \sqrt{F_1} \otimes I_E) \otimes |0\rangle_P\langle 0|_P.\end{aligned}$$

The motivation behind using our alternative formulation (9) is to prove later the convexity of the quantum conditional entropy (9) in terms of the parameters given in Eq. (3), so that we can use the convex optimization technique to find the minimum value of Eq. (9).

In order to calculate the key rate, we need to consider Eve's ambiguity on Alice's classical bit [7], [6] defined as follows. Let

$$\rho_{2,XEP} = \sum_{j=0,1} |j\rangle_A\langle j|_A \otimes I_{EP} \mathrm{Tr}_B[\rho_{2,ABEP}] |j\rangle_A\langle j|_A \otimes I_{EP}.$$

Eve's ambiguity on Alice's classical bit $S(X|EP)$ is defined as

$$S(X|EP) = S(\rho_{2,XEP}) - S(\rho_{2,EP}), \tag{9}$$

where $\rho_{2,EP} = \mathrm{Tr}_A[\rho_{2,XEP}]$, and $S(\cdot)$ denotes the von Neumann entropy.

In order to calculate the amount of public communication required for information reconciliation, we define the joint random variables (X', Y') as

$$\begin{aligned}X' &= j \text{ if the transmitted qubit is } |\varphi_j\rangle, \\ Y' &= k \text{ if the measurement outcome is } F_k,\end{aligned} \tag{10}$$

under the condition that the measurement outcome is either F_0 or F_1. Observe the difference between X and X'. X' is not defined but X is defined to be 0 when Bob's measurement outcome is either $F_{\bar{0}}$ or $F_{\bar{1}}$.

We shall show the asymptotic key rate per single transmitted qubit that is neither announced for the channel estimation nor discarded due to the measurement outcome being $F_{\bar{0}}$ or $F_{\bar{1}}$. Note that Eq. (9) is Eve's ambiguity per a qubit that is not announced for the channel estimation but *can be discarded*. The probability of the measurement outcome being F_0 or F_1 is

$$\mathrm{Tr}[\rho_{1,AB}(I_A \otimes (F_0 + F_1))].$$

So we can see that Eve's ambiguity per single transmitted qubit that is neither announced for the channel estimation nor discarded is

$$\frac{S(X|EP)}{\mathrm{Tr}[\rho_{1,AB}(I \otimes (F_0 + F_1))]}.$$

By [7], [6] the asymptotic key rate is

$$\frac{S(X|EP)}{\mathrm{Tr}[\rho_{1,AB}(I \otimes (F_0 + F_1))]} - H(X'|Y'). \tag{11}$$

Note that the above formula assumes that Alice and Bob knows the channel between them. In the BB92 protocol, we cannot estimate all the parameters of the channel. We can only estimate part of them. In Eq. (11) we can asymptotically determine the true values of $\mathrm{Tr}[\rho_{1,AB}(I \otimes (F_0 + F_1))]$ and $H(X'|Y')$. On the other hand we cannot know the true value of $S(X|EP)$. Therefore, we need to calculate the minimum value (i.e. the worst-case) of $S(X|EP)$ over all the possible quantum channel $\mathcal{E}_B$ between them.

One can compute the minimum of $S(X|EP)$ as follows. Observe first that $S(X|EP)$ is a function of the channel parameters Eq. (3) of $\mathcal{E}_B$. By the almost same argument as [9, Remark 11] one sees that $S(X|EP)$ is a convex function of the channel parameters Eq. (3). Moreover, we see that the minimum of $S(X|EP)$ is attained when $R_{xy} = R_{yx} = R_{yz} = R_{zy} = t_y = 0$ by the almost same argument as [9, Proposition 1]. Therefore, one can compute the minimization of $S(X|EP)$ by the convex optimization [3].

III. Numerical Result

We consider the depolarizing channel $\mathcal{E}_q$ with depolarizing rate q. The definition of q follows [8]. For a qubit density matrix ρ, we have $\mathcal{E}_q(\rho) = (1-q)\rho + (q/2)I_{2\times 2}$. With such a channel $\mathcal{E}_q$, R and $\vec{t}$ in Eq. (2) are given by

$$R = \begin{pmatrix} 1-4q/3 & 0 & 0 \\ 0 & 1-4q/3 & \\ 0 & 0 & 1-4q/3 \end{pmatrix}, \quad \vec{t} = \vec{0}.$$

Define

$$\rho_{1,AB,q} = (I \otimes \mathcal{E}_q)|\Psi\rangle\langle\Psi|.$$

Over $\mathcal{E}_q$ with infinitely many qubits, the asymptotic key rate is given by

$$\frac{\min S(X|EP)}{\mathrm{Tr}[\rho_{1,AB}(I \otimes (F_0 + F_1))]} - H(X'|Y'), \tag{12}$$

where the minimum is taken over the set of parameters in Eq. (3) such that

$$\begin{aligned}&\mathrm{Tr}[(|0\rangle\langle 0| \otimes F_0 + |1\rangle\langle 1| \otimes F_1)\rho_{1,AB}] \\ =\ &\mathrm{Tr}[(|0\rangle\langle 0| \otimes F_0 + |1\rangle\langle 1| \otimes F_1)\rho_{1,AB,q}], \qquad (13) \\ &\mathrm{Tr}[(|1\rangle\langle 1| \otimes F_0 + |0\rangle\langle 0| \otimes F_1)\rho_{1,AB}] \\ =\ &\mathrm{Tr}[(|1\rangle\langle 1| \otimes F_0 + |0\rangle\langle 0| \otimes F_1)\rho_{1,AB,q}]. \qquad (14)\end{aligned}$$

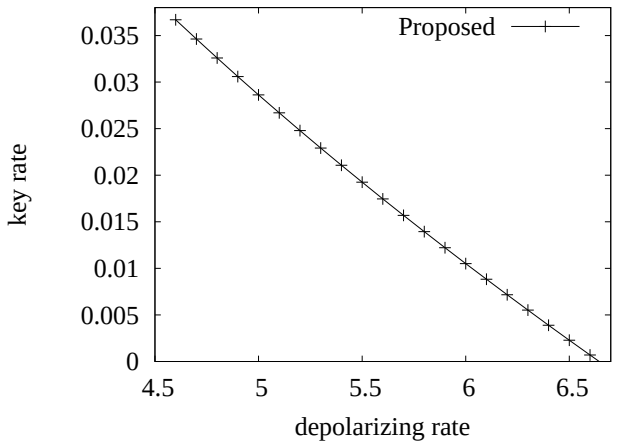

Fig. 1. Asymptotic Key Rate: The conventional methods [4], [7], [8] cannot generate key at depolarizing rate above 4.2% and they are not plotted.

We also required that parameters in Eq. (3) represent a completely positive map. We stress that we do not restrict the range of minimization to the depolarizing or the Pauli channels. The minimization is carried out over the set of all the qubit channels with (13) and (14).

The FindMinimum function in Mathematica 8.04 was used for the minimization. The program source code and the computation results are included in this eprint.

We only considered $\alpha = 0.39$ and did not optimized the value of α in Eq. (1). The key rate is plotted in Fig. 1. The convex optimization did not converge in 10^5 iterations when the depolarizing rate $\leq 4.5\%$. The key rate is plotted from depolarizing rate $\geq 4.6\%$.

IV. Conclusion

In this paper, we reformulated the secure key rate formula of the B92 protocol as a convex optimization. We have not resorted to skillful manipulation of inequalities, and the secure key rate is computed simply by a numerical optimization procedure. The result shows that the B92 protocol can securely generate key at significantly higher depolarizing rates than previous security analyzes.

Acknowledgment

The author would like to thank K. Azuma, G. Kato, K. Tamaki and T. Tsurumaru for helpful discussions. This research is partly supported by NICT and JSPS.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Intl. Conf. on Computers, Systems, and Signal Processing*, 1984, pp. 175–179.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[3] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[4] M. Christandl, R. Renner, and A. Ekert, "A generic security proof for quantum key distribution," Mar. 2004, arXiv:quant-ph/0402131.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2000.

[6] R. Renner, "Security of quantum key distribution," *International Journal on Quantum Information*, vol. 6, no. 1, pp. 1–127, Feb. 2008, arXiv:quant-ph/0512258 (originally published as Ph.D thesis, ETH Zürich, Switzerland, 2005).

[7] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, no. 1, p. 012332, Jul. 2005, arXiv:quant-ph/0502064.

[8] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Phys. Rev. Lett.*, vol. 90, no. 16, p. 167904, Apr. 2003, arXiv:quant-ph/0212162.

[9] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Phys. Rev. A*, vol. 78, no. 4, p. 042316, Oct. 2008, arXiv:0802.2419.